Exercises for Algebraic Number Theory Oliver Lorscheid
Series 4 Instituto Nacional de Matemática Pura e Aplicada
To hand in until 5.2.2015 with Emilio Peixoto Assemany or Roberto Alvarenga Jr.

Exercise 1.
Let $K = \mathbb{Q}[\sqrt{D}]$ be a quadratic number field. Determine a fundamental unit ϵ, i.e. a generator of $\mathcal{O}_K^\times$ modulo $\{\pm 1\}$, for $D = 2, 3, 5, 6, 7, 10$.

Exercise 2.
Let A be a Dedekind domain, K its fraction field, L/K a finite separable field extension of degree n. Show that B is a Dedekind domain.

Exercise 3.
Let A be a Dedekind domain, K its fraction field, L/K a finite separable field extension of degree n and B the integral closure of A in L. Show that there is for every ideal $I \subset B$ an element $b \in B$ such that the conductor of $A[b]$ is coprime to I and $L = K(b)$.

Exercise 4.
Let D be a squarefree integers different from 0 and 1 and let p be an odd prime number. Let $L = \mathbb{Q}(\sqrt{D})$ and B the integral closure of $\mathbb{Z}$ in L.

1. Let $\mathfrak{f}$ be the conductor of $\mathbb{Z}[\sqrt{D}]$. Show that $\gcd((p), \mathfrak{f}) = (1)$. What is $\gcd((2), \mathfrak{f}) = (1)$?
2. Show that
   - p ramifies in $\mathbb{Q}(\sqrt{D})$ if and only if $p | D$;
   - p splits in $\mathbb{Q}(\sqrt{D})$ if and only if $p \nmid D$ and $\left(\frac{D}{p}\right) = 1$;
   - p is inert in $\mathbb{Q}(\sqrt{D})$ if and only if $p \nmid D$ and $\left(\frac{D}{p}\right) = -1$.

   See Exercise 7 for the definition of the Legendre symbol $\left(\frac{D}{p}\right)$.

Exercise 5.
Let p be a prime number. Show that

- p ramifies in $\mathbb{Z}[i]$ if and only if $p = 2$;
- p splits in $\mathbb{Z}[i]$ if and only if $p \equiv 1 \pmod 4$;
- p is inert in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod 4$;

Compare this result with Exercise 4.

Exercise 6.

1. Show that $\mathbb{Z}[\sqrt[3]{2}]$ is the ring of algebraic integers of $\mathbb{Q}(\sqrt[3]{2})$.
2. What is the conductor of $\mathbb{Z}[\sqrt[3]{2}]$ (w.r.t. $\mathbb{Z}$)?
3. Determine the prime decompositions of the ideals $2B$, $3B$, $5B$ and $7B$ in $B = \mathbb{Z}[\sqrt[3]{2}]$.

Hint: Part 1 can be solved as follows. Let $\delta = \sqrt[3]{2}$. If $f = T^3 + c_2T^2 + c_1T + c_0$ is the minimal polynomial of an element $z = a + b\delta + c\delta^2 \in \mathbb{Q}(\delta)$ with $a, b, c \in \mathbb{Q}$, then $c_2 = 3a$, $c_1 = 3a^2 - 6bc$ and $c_0 = a^3 + 2b^3 + 4c^3 - 6abc$. Consider c_2, c_1, c_0 for z, δz and $\delta^2 z$ to show that $c_2, c_1, c_0 \in \mathbb{Z}$ only if $a, b, c \in \mathbb{Z}$.

***Exercise 7** (Legendre symbols)**.**
For an odd prime number p and $a \in \mathbb{Z}$, we define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } \bar{a} \text{ is a square in } \mathbb{F}_p^\times, \\ -1 & \text{if } \bar{a} \text{ is in } \mathbb{F}_p^\times, \text{ but not a square,} \\ 0 & \text{if } \bar{a} = 0 \text{ in } \mathbb{F}_p. \end{cases}$$

1. Show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for $a, b \in \mathbb{Z}$.
2. Show that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

***Exercise 8** (Gaussian reciprocity law)**.** Find as many different proofs as possible (in the literature) for the Gaussian reciprocity law:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

for two different odd prime numbers p and q.

***Exercise 9.**
Recall the proof of the main theorem of Galois theory.

The starred exercises are not to hand in.